

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF NEW YORK

---

PAUL D. CEGLIA,

Civil Action No. : 1:10-cv-00569-RJA

Plaintiff,

v.

DECLARATION  
OF  
JERRY GRANT

MARK ELLIOT ZUCKERBERG, Individually, and  
FACEBOOK, INC.

Defendants.

---

JERRY GRANT, submits this declaration and hereby declares under penalty of perjury and pursuant to 28 U.S.C. 1746 and under the laws of the United States that the following is true and correct:

1. I make this declaration upon personal knowledge.
2. I am a Certified AccessData Forensic Examiner
3. I have more than 25 years of professional computer forensic expert and systems analysis experience.
4. I am currently a Computer Forensic Investigator for the Western District of New York Federal Public Defender's Office. I'm also an independent forensic examiner involved in other cases.
5. I perform forensic investigations on electronic evidence involved in Federal Criminal Cases as well as State Cases.
6. I have lectured and conducting training programs for many large groups at various companies and have received various certificates in forensics,

specialized computer training and programming. I have lectured at a number of local and national computer forensics conferences.

7. Lectured on numerous technical subjects including DOS and Windows file systems, architecture and the boot process, DOS and Windows examination techniques and procedures, recovery of deleted files, date and time stamp definitions / alterations, recovering formatted disks, the process and problems in making duplicate copies of media, file type identification and the use of file viewing applications during examinations, archived files and compressed disks, data format conversion, and the examination of Windows swap and related files.
8. I have experience in all aspects of personal computers including the following:
  - a. Extensive knowledge of DOS and all versions of Windows Operating System
  - b. Extensive knowledge and experience with popular software applications
  - c. Extensive knowledge of computer hardware and configurations
  - d. Extensive knowledge with the technical workings of a computer hard drive
  - e. Extensive knowledge on cell site information and cell phone forensics
9. On Thursday, March 31, 2011, I received 41 floppy disks for review. On Friday, April 1, 2011, I created forensically sound, bit by bit, images of each for analysis.
10. Following the creation of the forensic copies, I performed an initial review of the diskettes and determined that the first 2 were relevant to this matter. I

further analyzed the 2 relevant disks to determine the dates and times that various documents on those disks were created.

11. In addition, I analyzed those disks specifically examining them for the following forensically relevant items:

a. File Allocation Tables (FAT 12)

- i. The File allocation Table is the area of the drive that contains the name, date and location of files on the floppy disk (similar to the table of contents of a book). This is reviewed to compare the contents of the actual files that exist to the names in the FAT for discrepancies. It is also reviewed to determine if any residual information exists indicating duplicate files and or the names of previously deleted files that might be of interest. In this case nothing was located that would indicate fraud.

b. File Dates/Times (Created, Modified Accessed)

- i. The File dates/times are the actual dates/times on the physical files that reside on the floppy disk. These are compared to any internal dates found within the document content themselves to determine if there are any discrepancies. This is used to determine if the content matches the timeframe that the files were created and/or edited. In this case, no discrepancies existed that would indicate fraud.

c. Metadata Dates/Times (Created, Modified, Accessed, Printed)

- i. Like the file dates/time, Metadata dates/times are internal to the document and do not change if a document is copied from one device to

another. The are reviewed and compared to the File Dates/Times as well to determine the sequence of events. In this case nothing was located that would indicate fraud.

d. Total Edited Time Metadata Field

- i. This field is part of the internal Metadata of the document and is updated by the Word Processing program that is used to create/edit the document. The field was reviewed to determine the actual time spent editing the content. In this case, the content of the documents was large compared to the logged editing time which is consistent with the pasting of data from the clipboard instead of typing or manually editing the content.

e. All Other Metadata fields

- i. Any additional fields that contain data are reviewed for additional information related to the origin of document and/or the machine created on. In this case additional information on other computers, users and companies was located, but nothing was found indicating fraud.

f. Fonts Used

- i. The font types are reviewed and compared to the fonts available at the time of the create/modify date of the document. This is done to determine if the document was created at a later date and the actual file and metadata dates were false. In this case all fonts were correct and

nothing indicated any signs of fraud.

g. Allocated Space

- i. The allocated space is the space that is taken up on the floppy disk from existing files. This is reviewed to determine what parts of the actual floppy disk the data resides on as well as to determine if any hidden or encrypted data exists. In this case nothing was located to indicate any fraud.

h. Unallocated Space

- i. The unallocated space is the space that may contain data from previously deleted files. It is examined to review deleted data and to perform keyword searches for the content of deleted files. This is also done to look for any forensic artifacts of a file wiping process or to locate relevant data for comparison. In this case nothing was found that would indicate any fraud.

i. Slack Space

- i. The Slack Space is similar to the unallocated space but is the leftover data from another file that is at the end of an existing file. This is similar to a 2 hour movie on a VCR tape that was overwritten by a 1 hour movie. The first hour of the tape is the new movie but the last hour is the leftover last half of the old movie. This is examined to look for pieces of deleted data to compare to the actual files on the floppy disk to uncover evidence of file versions/editing. In this case, nothing was

found to indicate that.

j. Temporary Files

- i. The temporary files are those that are created during the editing/printing of a document. These are then normally deleted after the document is saved or printed. These were reviewed, similar to the remnants of the slack space, to look for evidence of versions and/or editing. In this case, nothing was found to indicate other edited versions of any document relevant to fraud.

k. Carved Files

- i. The carved files are the files/remnants that were deleted on the floppy disk but could be recovered. These were reviewed like the Slack Space and Temporary Files for evidence of file versions and editing. In this case, nothing was found to indicate fraud.

l. Carved Folders

- i. Carved folders are folders that were once deleted but could be recovered similar to the carved files. Recovering a folder could uncover evidence of the actual files that once existed in them for comparison like the other processes. In this case, nothing was found to indicate fraud.

m. File Header Information

- i. The file header information is the beginning of a file that is unique and determines the type of document (Word 97, Rich Text, etc). These were compared to the versions of software that existed on the date/time the

document was created. This is done to determine if the file was created with a program that did not exist at that time indicating fraud. In this case, all file headers matched the available versions of the programs at that time so nothing was found to indicate fraud.

- n. File Comparisons for changes
  - i. I compared files with the same and/or similar names to determine if they were exact. This was done to determine if there were multiple versions of the files or slightly modified versions that would indicate manipulation. In this case nothing was found to indicate fraud.
- o. Versions of Programs/Documents (Word 97, Word 2002, Word 6.0, Microsoft RTF, Works 5.0)
  - i. Similar to comparing the File Header Information, the versions of the programs indicated by the headers were compared to make sure they did indeed exist at the date/time of the file creation. The programs matched the header information, so in this case nothing was found to indicate fraud.
- p. OLE Streams (Individual Components of Documents)
  - i. The OLE Streams are individual parts of a file/document within the file itself. These were reviewed to compared the types of OLE that existed at the time and to match them to the programs used. In this case, nothing was found to indicate fraud.
- q. 0 Length Files (Remnants of deleted files)

- i. The 0 Length Files are names of deleted files that were leftover in the File Allocation Table. These items are individually carved to recover any dates and/or information for comparison. In this case, nothing was found to indicate fraud.
- r. Pasted E-Mail header contents
  - i. I compared the portions of the pasted e-mails that contained actual e-mail header information. This would be the underlying information that the e-mail servers would use to actually deliver the e-mail. This was compared to determine if the format, and information pasted, matched a true e-mail header format. In this case, they appear to be formatted properly and nothing was found to indicate fraud.
- s. RTF Specification Versions and Dates
  - i. The RTF Specification is the blueprint of the Rich Text Format files that were located on the floppy disks. I reviewed the actual versions of the file format that existed at the time the files were created. This was done similar to comparison to the versions of the software used to determine if the physical structure of the file matched the specification out at the time. In this case, nothing was found to indicate fraud.
- t. DOC Binary File Format Specification Versions and Dates
  - i. Similar to the RTF Specification, one exists for the DOC files (Microsoft Word). This was reviewed and compared to the existing files on the floppy disks and in this case, nothing was found to indicate fraud.

I hereby and hereby declare under penalty of perjury and pursuant to 28 U.S.C. 1746 and under the laws of the United States that the following is true and correct:

DATED: November 16, 2011.

  
Declarant